


 Searching within **The ACM Digital Library** for: feistel and block cipher ([start a new search](#))

Found 25 of 270,768

## REFINER YOUR SEARCH

[Search Results](#) • [Related Journals](#) • [Related Magazines](#) • [Related SIGs](#)
[Related Conferences](#)

## Refine by Keywords

feistel and block cipher

Discovered Terms

SEARCH

## Refine by People

[Names](#)  
[Institutions](#)  
[Authors](#)  
[Reviewers](#)

## Refine by Publications

[Publication Year](#)  
[Publication Names](#)  
[ACM Publications](#)  
[All Publications](#)  
[Content Formats](#)  
[Publishers](#)

## Refine by Conferences

[Sponsors](#)  
[Events](#)  
[Proceeding Series](#)

## ADVANCED SEARCH

[Advanced Search](#)

## FEEDBACK

Please provide us with feedback

Found 25 of 270,768

Results 1 - 20 of 25

 Sort by  in 

Save results to a Binder

Result page: 1 [2](#) [next](#) [>>](#)

- 1 [Review of "Codes: The Guide to Secrecy from Ancient to Modern Times by Richard A. Mollin". Chapman & Hall/CRC, 2005](#)

Adam Bender

 March 2006  
**Publisher:** ACM

Full text available: Pdf (124.80 KB)

 Additional Information: [full citation](#), [references](#), [index terms](#)
**Bibliometrics:** Downloads (6 Weeks): 0, Downloads (12 Months): 17, Downloads (Overall): 160, Citation Count: 0

- 2 [Security in outsourcing of association rule mining](#)

W. K. Wong, David W. Cheung, Edward Hung, Ben Kao, Nikos Mamoulis

 September 2007  
**Publisher:** VLDB Endowment

Full text available: Pdf (319.84 KB)

 Additional Information: [full citation](#), [abstract](#), [references](#)
**Bibliometrics:** Downloads (6 Weeks): 22, Downloads (12 Months): 120, Downloads (Overall): 339, Citation Count: 1

Outsourcing association rule mining to an outside service provider brings several important benefits to the data owner. These include (i) relief from the high mining cost, (ii) minimization of demands in resources, and (iii) effective centralized mining ...

- 3 [Survey and benchmark of block ciphers for wireless sensor networks](#)

Yee Wei Law, Jeroen Doumen, Pieter Hartel

 February 2006  
**Publisher:** ACM [Request Permissions](#)

Full text available: Pdf (354.39 KB)

 Additional Information: [full citation](#), [appendices and supplements](#), [abstract](#), [references](#), [index terms](#)
**Bibliometrics:** Downloads (6 Weeks): 32, Downloads (12 Months): 309, Downloads (Overall): 2162, Citation Count: 10

Cryptographic algorithms play an important role in the security architecture of wireless sensor networks (WSNs). Choosing the most storage- and energy-efficient block cipher is essential, due to the facts that these networks are meant to operate without ...


**Keywords:** Sensor networks, block ciphers, cryptography, energy efficiency

#### 4 [Hardware and Binary Modification Support for Code Pointer Protection From Buffer Overflow](#)

[Nathan Tuck](#), [Brad Calder](#), [George Varghese](#)

December **MI CRO 37: Proceedings of the 37th annual IEEE/ACM International Symposium on 2004** Microarchitecture

**Publisher:** IEEE Computer Society

Full text available:  [PDF](#) (294.15 KB)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#)

**Bibliometrics:** Downloads (6 Weeks): 5, Downloads (12 Months): 48, Downloads (Overall): 458, Citation Count: 15


Buffer overflow vulnerabilities are currently the most prevalent security vulnerability; they are responsible for over half of the CERT advisories issued in the last three years. Since many attacks exploit buffer overflow vulnerabilities, techniques that ...

#### 5 [Versatile padding schemes for joint signature and encryption](#)

 [Yevgeniy Dodis](#), [Michael J. Freedman](#), [Stanislaw Jarecki](#), [Shabsi Waikish](#)

October **CCS '04: Proceedings of the 11th ACM conference on Computer and communications security 2004**

**Publisher:** ACM 

Full text available:  [PDF](#) (203.91 KB)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 6, Downloads (12 Months): 51, Downloads (Overall): 563, Citation Count: 1

We propose several highly-practical and optimized constructions for joint signature and encryption primitives often referred to as  $\langle \text{signcrypt} \rangle$ . All our signcrypt schemes, built directly from trapdoor permutations such as RSA, share ...


**Keywords:** extractable commitments, feistel transform, joint signature and encryption, signcrypt, universal padding schemes

#### 6 [Proofs of retrievability: theory and implementation](#)

 [Kevin D. Bowers](#), [Ari Juels](#), [Alina Oprea](#)

November 2009 **CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security**

**Publisher:** ACM 

Full text available:  [PDF](#) (538.44 KB)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 48, Downloads (12 Months): 84, Downloads (Overall): 84, Citation Count: 0

A *proof of retrievability* (POR) is a compact proof by a file system (prover) to a client (verifier) that a target file  $F$  is intact, in the sense that the client can fully recover it. As PORs incur lower communication complexity than transmission ...


**Keywords:** cloud storage, data availability, erasure codes, proofs of retrievability

#### 7 [Energy evaluation of software implementations of block ciphers under memory constraints](#)

[Johann Großschädl](#), [Stefan Tillich](#), [Christian Rechberger](#), [Michael Holmann](#), [Marcel Medwed](#)

April **DATE '07: Proceedings of the conference on Design, automation and test in Europe 2007**

**Publisher:** EDA Consortium

Full text available:  [PDF](#) (262.13 KB)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#)

**Bibliometrics:** Downloads (6 Weeks): 2, Downloads (12 Months): 75, Downloads (Overall): 261, Citation Count: 1

Software implementations of modern block ciphers often require large lookup tables along with code size increasing optimizations like loop unrolling to reach peak performance on general-purpose processors. Therefore, block ciphers are difficult to implement ...

**Keywords:** code size reduction, energy optimization, lightweight cryptography, memory footprint, symmetric cipher

8 [Battery power-aware encryption](#)

R. Chandramouli, S. Bapatia, K. P. Subbalakshmi, R. N. Uma

May **Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 2  
2006Publisher: ACM [Request Permissions](#)Full text available: [PDF](#) (454.71 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 146, Downloads (Overall): 831, Citation Count: 2

Minimizing power consumption is crucial in battery power-limited secure wireless mobile networks. In this paper, we (a) introduce a hardware/software set-up to measure the battery power consumption of encryption algorithms through real-life experimentation, ...

**Keywords:** Low-power encryption, optimization, profiling

9 [ASIP architecture exploration for efficient IPsec encryption: A case study](#)

Hans Scharwaechter, David Kammer, Andreas Wiefenik, Manuel Hohenauer, Kingshuk Karuri, Jianliang Ceng, Rainer Leupers, Gerd Ascheid, Heinrich Meyr

May **Transactions on Embedded Computing Systems (TECS)**, Volume 6 Issue 2  
2007Publisher: ACM [Request Permissions](#)Full text available: [PDF](#) (393.57 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 119, Downloads (Overall): 480, Citation Count: 1

Application-Specific Instruction-Set Processors (ASIPs) are becoming increasingly popular in the world of customized, application-driven *System-on-Chip* (SoC) designs. Efficient ASIP design requires an iterative architecture exploration loop---gradual ...

**Keywords:** ADL, ASIP, IPsec, computer-aided design

10 [Design and evaluation of lightweight middleware for personal wireless body area network](#)

Augustinus Borgy Waluyo, Isaac Peik, Xiang Chen, Wee-Soon Yeoh

October **Personal and Ubiquitous Computing**, Volume 13 Issue 7  
2009

Publisher: Springer-Verlag

Full text available: [PDF](#) (1.07 MB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 35, Downloads (12 Months): 118, Downloads (Overall): 118, Citation Count: 0

This paper presents a lightweight middleware to be used for wireless medical body area networks. The middleware is designed to reside in mobile devices, and acts as a gateway to receive sensor data as well as to control a set of sensor devices attached ...

**Keywords:** Lightweight middleware, Mobile middleware, Wireless body area network middleware

11 [Efficient and provably secure ciphers for storage device block level encryption](#)

Yuliang Zheng, Yongge Wang

November **StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability**  
2005Publisher: ACM [Request Permissions](#)Full text available: [PDF](#) (85.22 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 32, Downloads (Overall): 185, Citation Count: 0

Block ciphers generally have fixed and relatively small input length. Thus they are often used in some mode of operations (e.g., ECB, CBC, CFB, and CTR) that enables the encryption of longer messages. Unfortunately, all these modes of operation reveal ...

**Keywords:** hash function, storage device encryption, symmetric cipher

12 [Enhancing lifetime and security of PCM-based main memory with start-gap wear leveling](#)

Moinuddin K. Oureshi, John Karidis, Michele Franceschini, Vijayalakshmi Srinivasan, Luis Lastras, Bulent Abali  
December 2009 **Micro-42: Proceedings of the 42nd Annual IEEE/ACM International Symposium on Microarchitecture**

**Publisher:** ACM [Request Permissions](#)

Full text available: [Pdf](#) (1.28 MB)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 45, Downloads (12 Months): 45, Downloads (Overall): 45, Citation Count: 0

Phase Change Memory (PCM) is an emerging memory technology that can increase main memory capacity in a cost-effective and power-efficient manner. However, PCM cells can endure only a maximum of  $10^7$  -  $10^8$  writes, making a PCM based ...

**Keywords:** endurance, phase change memory, wear leveling

13 [A low-resource public-key identification scheme for RFID tags and sensor nodes](#)

Yossef Oren, Martin Feidhofer

March 2009 **WiSec '09: Proceedings of the second ACM conference on Wireless network security**

**Publisher:** ACM [Request Permissions](#)

Full text available: [Pdf](#) (552.89 KB)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 32, Downloads (12 Months): 309, Downloads (Overall): 309, Citation Count: 0

We revisit a public key scheme presented by Shamir in [19] (and simultaneously by Naccache in [15]) and examine its applicability for general-purpose RFID tags in the supply chain. Using a combination of new and established space-saving methods, we present ...

**Keywords:** hardware implementation, public-key encryption, rabin encryption, rfid technology

14 [Elastic block ciphers: the basic design](#)

Debra Cook, Angelos Keromytis, Moti Yung

March 2007 **ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security**

**Publisher:** ACM [Request Permissions](#)

Full text available: [Pdf](#) (146.57 KB)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 3, Downloads (12 Months): 43, Downloads (Overall): 216, Citation Count: 1

We introduce the concept of an *elastic block cipher*, which refers to stretching the supported block size of a block cipher to any length up to twice the original block size while incurring a computational workload that is proportional to the block ...

**Keywords:** block ciphers, elastic block ciphers, encryption, variable-length block ciphers

15 [Technical opinion: designing cryptography for the new century](#)

Susan Landau

May 2000 **Communications of the ACM**, Volume 43 Issue 5

**Publisher:** ACM [Request Permissions](#)

Full text available: [Html](#) (35.06 KB), [Pdf](#) (215.10 KB)

**Additional Information:** [full citation](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 9, Downloads (12 Months): 97, Downloads (Overall): 1252, Citation Count: 1

16 [Cryptanalysis of four-rounded DES using binary particleswarm optimization](#)
 Waseem Shahzad, Abdul Basit Siddiqui, Farrukh Aslam Khan


 July **GECCO '09: Proceedings of the 11th Annual Conference Companion on Genetic and Evolutionary 2009** Computation Conference: Late Breaking Papers


Publisher: ACM

Full text available:  Pdf (452.35 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 62, Downloads (Overall): 62, Citation Count: 0


Cryptanalysis of feistel ciphers is difficult due to their high nonlinearity and autocorrelation. On the other hand, substitution ciphers are easily breakable due to their simpler encryption process. In this paper, a highly efficient Binary Particle ...

**Keywords:** cryptanalysis, des, fitness function, ga, pso
17 [High performance encryption cores for 3G networks](#)
 Tomás Balderas-Contreras, René Cumplido

 June 2005 **DAC '05: Proceedings of the 42nd annual Design Automation Conference**
Publisher: ACM Full text available:  Pdf (869.33 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 47, Downloads (Overall): 454, Citation Count: 0

This paper presents two novel and high performance hardware architectures, implemented in FPGA technology, for the KASUMI block cipher; this algorithm lies at the core of the confidentiality and integrity algorithms defined for the Universal Mobile Telecommunication ...


**Keywords:** 3G, FPGA, KASUMI, UMTS security architecture
18 [Review of Coding theory and cryptography: the essentials, second edition, revised and expanded by D.R. Hankerson, et al. Marcel Dekker, 2000.](#)
 Robert J. Irwin

 December **SI GACT News** , Volume 34 Issue 4  
2003

Publisher: ACM


Full text available:  Pdf (73.81 KB)Additional Information: [full citation](#), [references](#)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 30, Downloads (Overall): 453, Citation Count: 0

19 [Cryptanalysis of four-rounded DES using binary particle swarm optimization](#)
 Waseem Shahzad, Abdul Basit Siddiqui, Farrukh Aslam Khan

 July **GECCO '09: Proceedings of the 11th Annual conference on Genetic and evolutionary computation 2009**

Publisher: ACM

Full text available:  Pdf (353.56 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 50, Downloads (Overall): 50, Citation Count: 0

A highly efficient Binary PSO based cryptanalysis approach for four-rounded DES is presented. Several optimum keys are generated in different runs of the algorithm on the basis of their fitness value and finally, the real key is found by guessing every ...

**Keywords:** DES, GA, PSO, cryptanalysis, fitness function

## 20 [Programming by sketching for bit-streaming programs](#)



[Armando Solar-Lezama](#), [Rodric Rabbah](#), [Pavlos P. Bessis](#), [Kemal Ebcioglu](#)

June 2005 **PLDI '05: Proceedings of the 2005 ACM SIGPLAN conference on Programming language design and implementation**

Publisher: ACM [Request Permissions](#)

Full text available: [Pdf \(320.08 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 6, Downloads (12 Months): 70, Downloads (Overall): 424, Citation Count: 7

This paper introduces the concept of *programming with sketches*, an approach for the rapid development of high-performance applications. This approach allows a programmer to write clean and portable reference code, and then obtain a high-quality ...

**Keywords:** StreamIt, domain specific compiler, domain specific language, sketching, stream programming, synchronous dataflow

Also published in:

June 2005 **SIGPLAN Notices** Volume 40 Issue 6

Result page: 1 [2](#) [next](#)  
[»»](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2010 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)